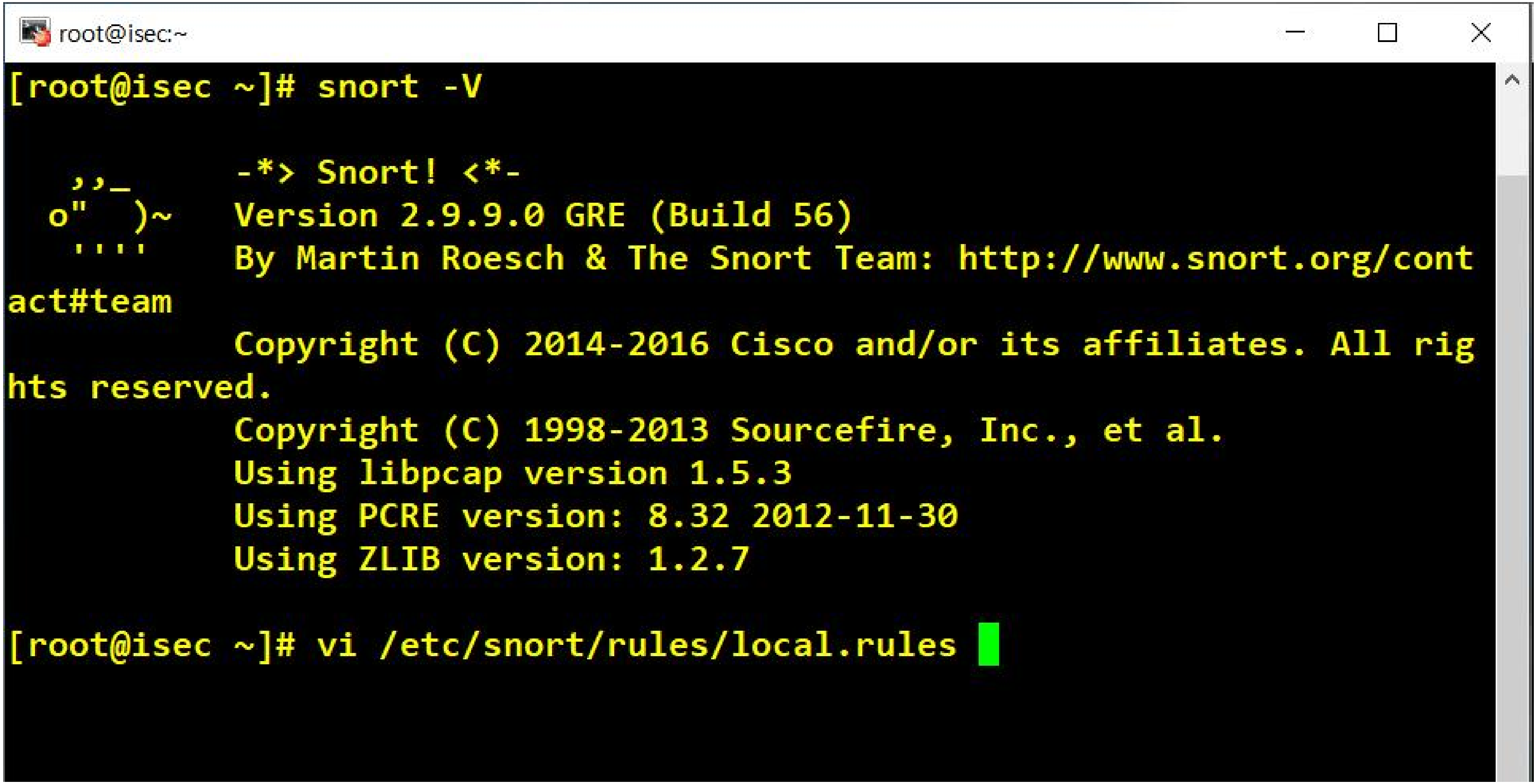
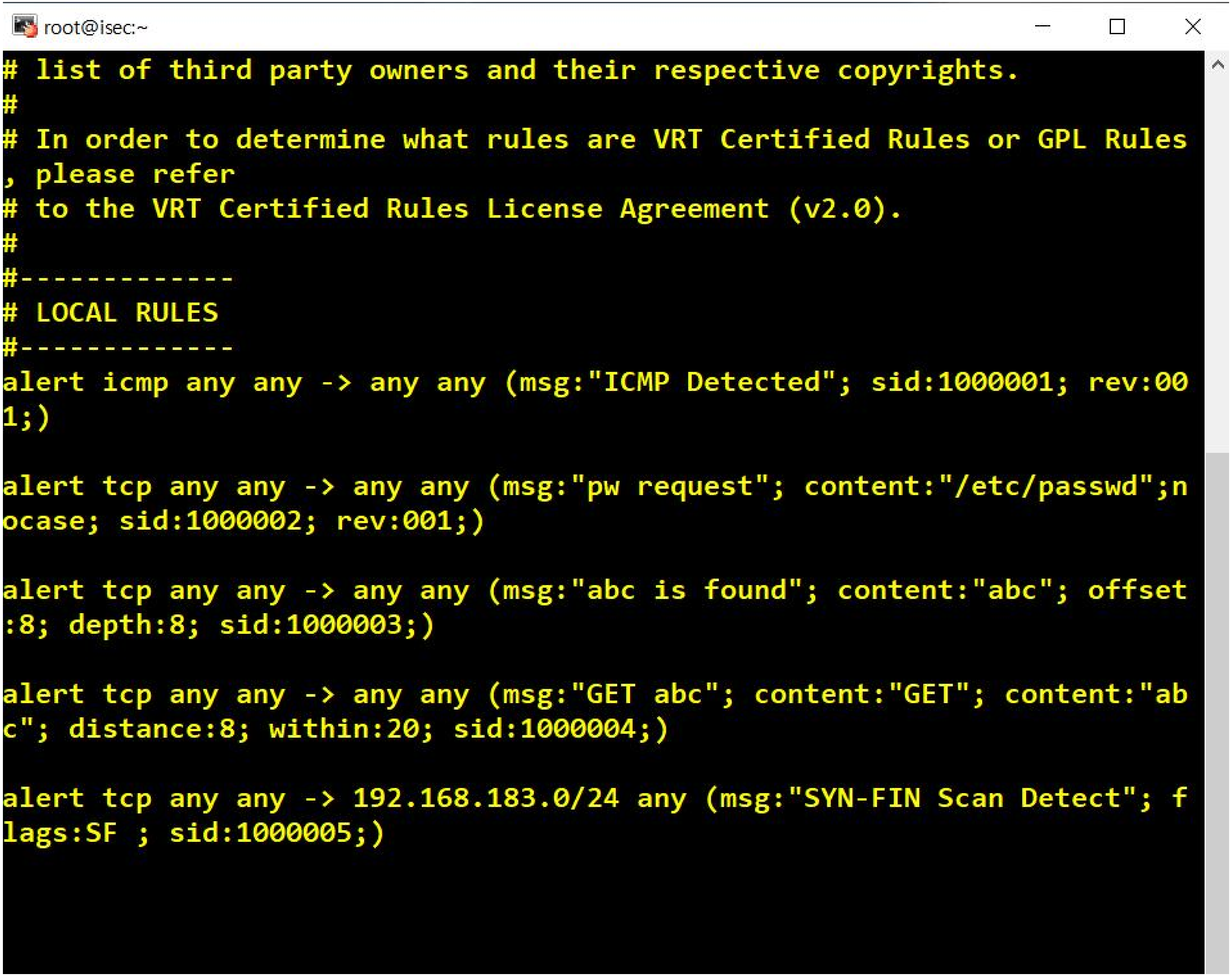
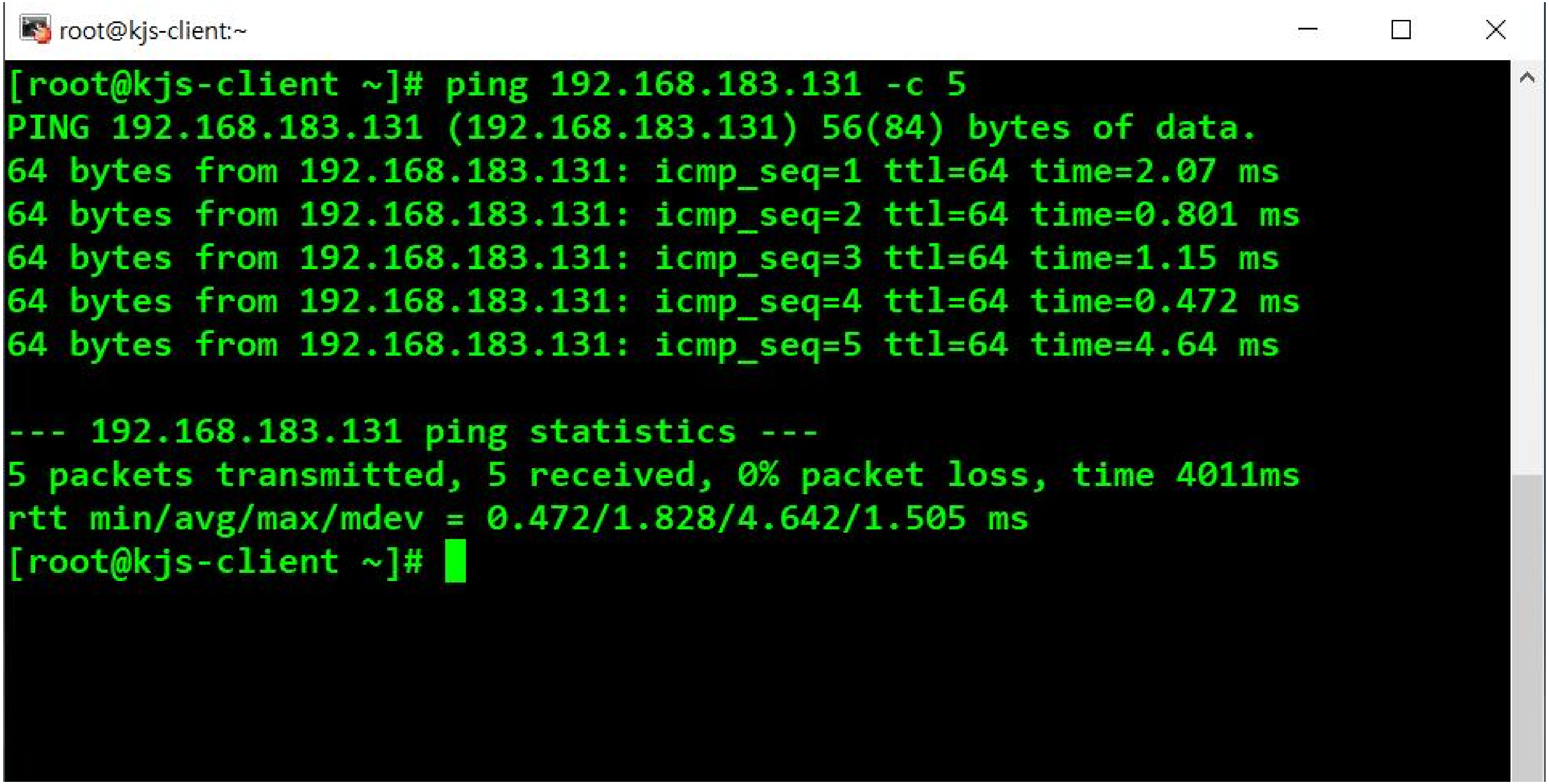


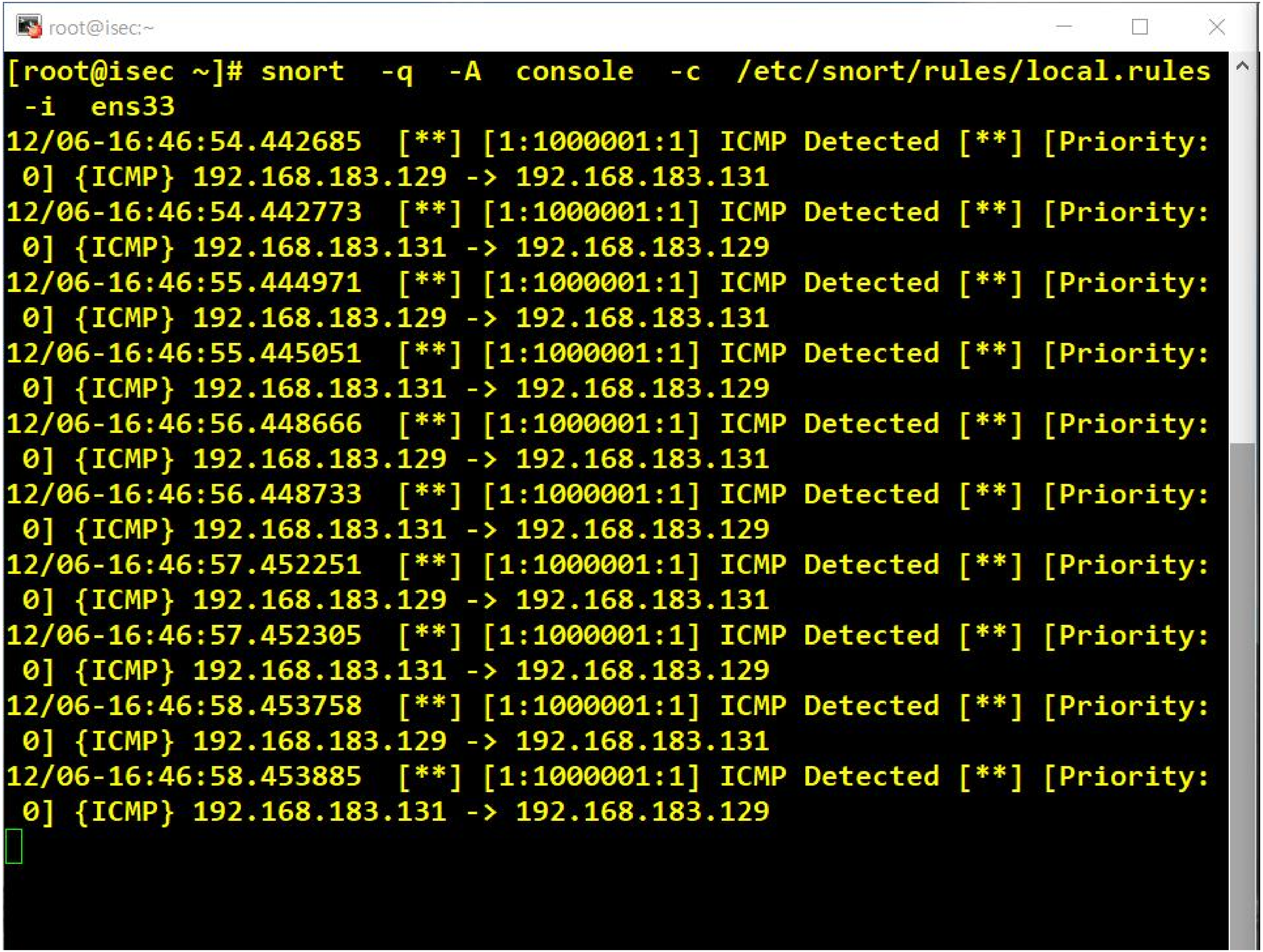
```
[root@isec ~]# snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.9.0 GRE (Build 56)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/cont
act#team
           Copyright (C) 2014-2016 Cisco and/or its affiliates. All rig
hts reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.5.3
           Using PCRE version: 8.32 2012-11-30
           Using ZLIB version: 1.2.7

[root@isec ~]# vi /etc/snort/rules/local.rules
```



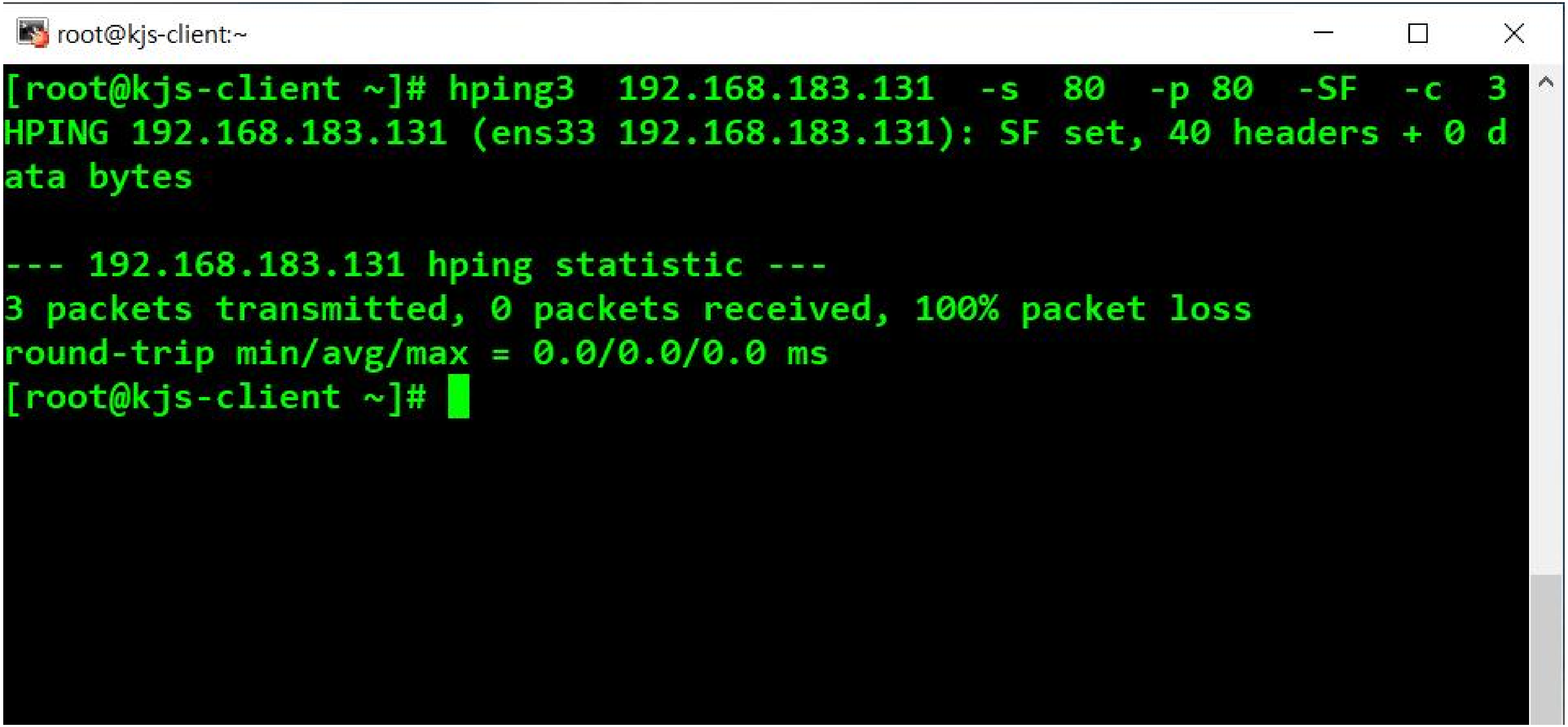
```
# list of third party owners and their respective copyrights.
#
# In order to determine what rules are VRT Certified Rules or GPL Rules
, please refer
# to the VRT Certified Rules License Agreement (v2.0).
#
#-------------
# LOCAL RULES
#-------------
alert icmp any any -> any any (msg:"ICMP Detected"; sid:1000001; rev:00
1;)

alert tcp any any -> any any (msg:"pw request"; content:"/etc/passwd";n
ocase; sid:1000002; rev:001;)

alert tcp any any -> any any (msg:"abc is found"; content:"abc"; offset
:8; depth:8; sid:1000003;)

alert tcp any any -> any any (msg:"GET abc"; content:"GET"; content:"ab
c"; distance:8; within:20; sid:1000004;)

alert tcp any any -> 192.168.183.0/24 any (msg:"SYN-FIN Scan Detect"; f
lags:SF ; sid:1000005;)
```



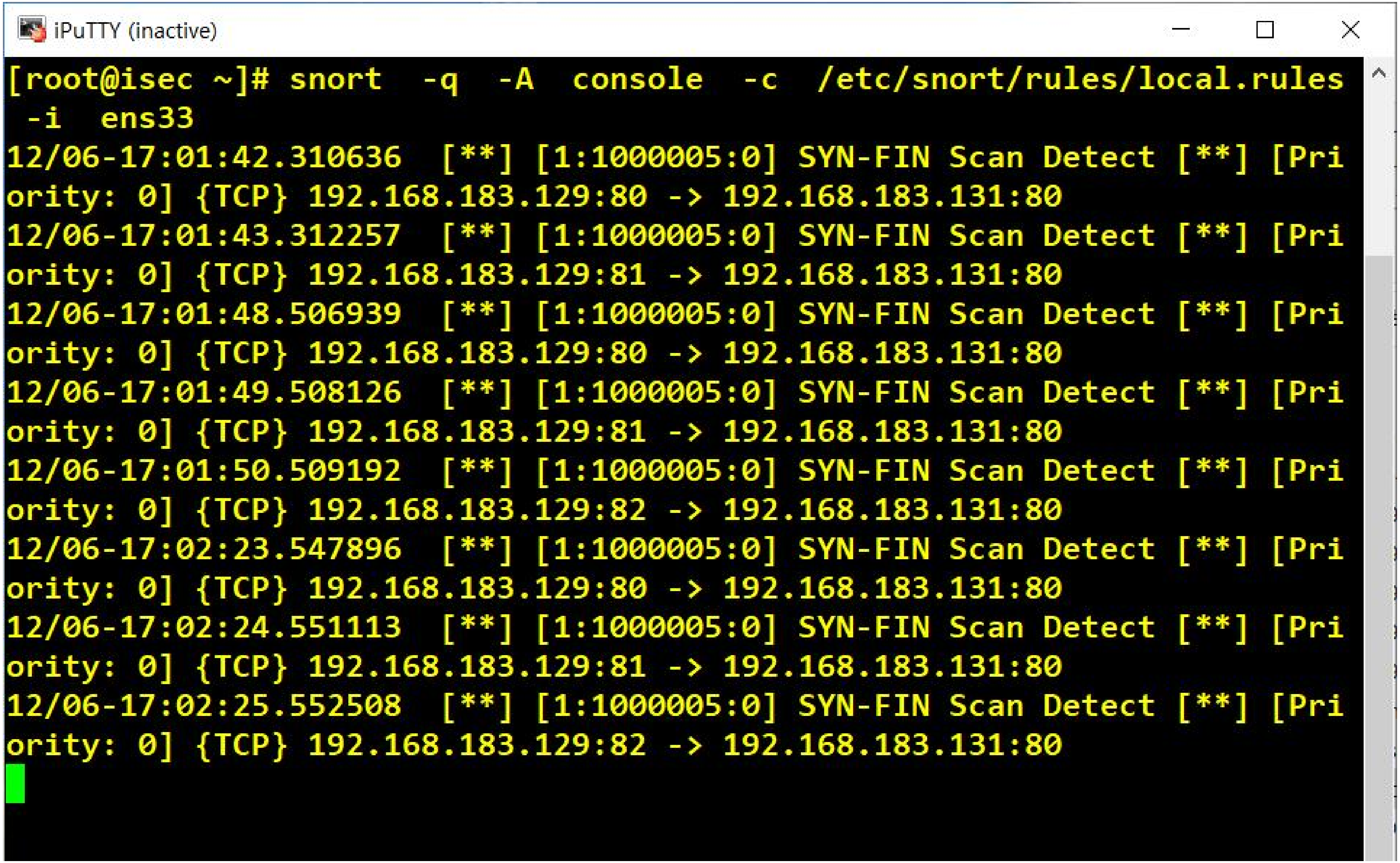
```
[root@kjs-client ~]# ping 192.168.183.131 -c 5
PING 192.168.183.131 (192.168.183.131) 56(84) bytes of data.
64 bytes from 192.168.183.131: icmp_seq=1 ttl=64 time=2.07 ms
64 bytes from 192.168.183.131: icmp_seq=2 ttl=64 time=0.801 ms
64 bytes from 192.168.183.131: icmp_seq=3 ttl=64 time=1.15 ms
64 bytes from 192.168.183.131: icmp_seq=4 ttl=64 time=0.472 ms
64 bytes from 192.168.183.131: icmp_seq=5 ttl=64 time=4.64 ms

--- 192.168.183.131 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4011ms
rtt min/avg/max/mdev = 0.472/1.828/4.642/1.505 ms
[root@kjs-client ~]# 
```



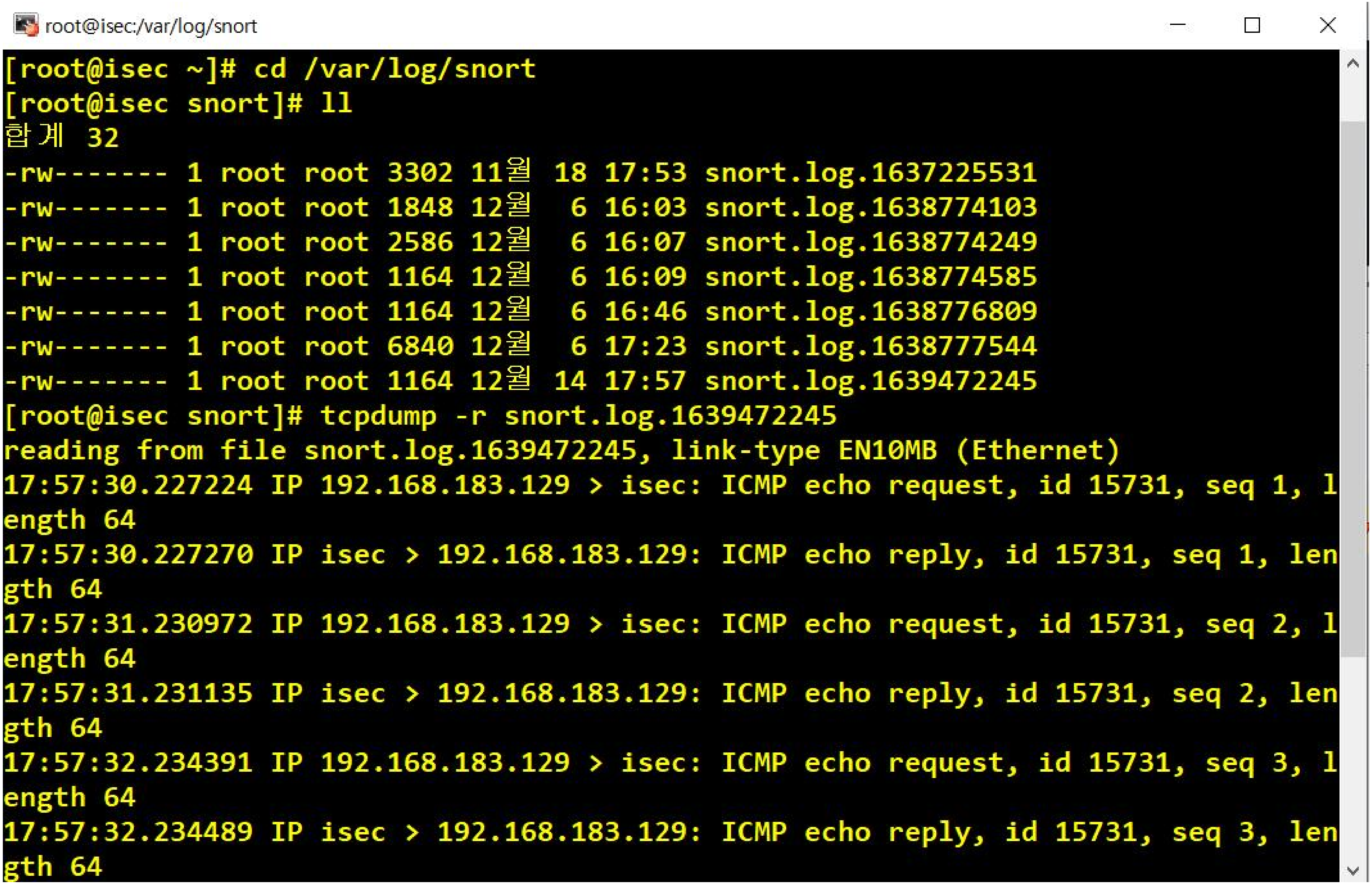
```
[root@isec ~]# snort  -q  -A  console  -c  /etc/snort/rules/local.rules
 -i  ens33
12/06-16:46:54.442685  [**] [1:1000001:1] ICMP Detected [**] [Priority:
 0] {ICMP} 192.168.183.129 -> 192.168.183.131
12/06-16:46:54.442773  [**] [1:1000001:1] ICMP Detected [**] [Priority:
 0] {ICMP} 192.168.183.131 -> 192.168.183.129
12/06-16:46:55.444971  [**] [1:1000001:1] ICMP Detected [**] [Priority:
 0] {ICMP} 192.168.183.129 -> 192.168.183.131
12/06-16:46:55.445051  [**] [1:1000001:1] ICMP Detected [**] [Priority:
 0] {ICMP} 192.168.183.131 -> 192.168.183.129
12/06-16:46:56.448666  [**] [1:1000001:1] ICMP Detected [**] [Priority:
 0] {ICMP} 192.168.183.129 -> 192.168.183.131
12/06-16:46:56.448733  [**] [1:1000001:1] ICMP Detected [**] [Priority:
 0] {ICMP} 192.168.183.131 -> 192.168.183.129
12/06-16:46:57.452251  [**] [1:1000001:1] ICMP Detected [**] [Priority:
 0] {ICMP} 192.168.183.129 -> 192.168.183.131
12/06-16:46:57.452305  [**] [1:1000001:1] ICMP Detected [**] [Priority:
 0] {ICMP} 192.168.183.131 -> 192.168.183.129
12/06-16:46:58.453758  [**] [1:1000001:1] ICMP Detected [**] [Priority:
 0] {ICMP} 192.168.183.129 -> 192.168.183.131
12/06-16:46:58.453885  [**] [1:1000001:1] ICMP Detected [**] [Priority:
 0] {ICMP} 192.168.183.131 -> 192.168.183.129
```



```
[root@kjs-client ~]# hping3  192.168.183.131  -s  80  -p 80  -SF  -c  3
HPING 192.168.183.131 (ens33 192.168.183.131): SF set, 40 headers + 0 d
ata bytes

--- 192.168.183.131 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@kjs-client ~]# 
```



```
[root@isec ~]# snort  -q  -A  console  -c  /etc/snort/rules/local.rules
 -i  ens33
12/06-17:01:42.310636  [**] [1:1000005:0] SYN-FIN Scan Detect [**] [Pri
ority: 0] {TCP} 192.168.183.129:80 -> 192.168.183.131:80
12/06-17:01:43.312257  [**] [1:1000005:0] SYN-FIN Scan Detect [**] [Pri
ority: 0] {TCP} 192.168.183.129:81 -> 192.168.183.131:80
12/06-17:01:48.506939  [**] [1:1000005:0] SYN-FIN Scan Detect [**] [Pri
ority: 0] {TCP} 192.168.183.129:80 -> 192.168.183.131:80
12/06-17:01:49.508126  [**] [1:1000005:0] SYN-FIN Scan Detect [**] [Pri
ority: 0] {TCP} 192.168.183.129:81 -> 192.168.183.131:80
12/06-17:01:50.509192  [**] [1:1000005:0] SYN-FIN Scan Detect [**] [Pri
ority: 0] {TCP} 192.168.183.129:82 -> 192.168.183.131:80
12/06-17:02:23.547896  [**] [1:1000005:0] SYN-FIN Scan Detect [**] [Pri
ority: 0] {TCP} 192.168.183.129:80 -> 192.168.183.131:80
12/06-17:02:24.551113  [**] [1:1000005:0] SYN-FIN Scan Detect [**] [Pri
ority: 0] {TCP} 192.168.183.129:81 -> 192.168.183.131:80
12/06-17:02:25.552508  [**] [1:1000005:0] SYN-FIN Scan Detect [**] [Pri
ority: 0] {TCP} 192.168.183.129:82 -> 192.168.183.131:80
```



```
[root@isec ~]# cd /var/log/snort
[root@isec snort]# ll
합계 32
-rw------- 1 root root 3302 11월 18 17:53 snort.log.1637225531
-rw------- 1 root root 1848 12월  6 16:03 snort.log.1638774103
-rw------- 1 root root 2586 12월  6 16:07 snort.log.1638774249
-rw------- 1 root root 1164 12월  6 16:09 snort.log.1638774585
-rw------- 1 root root 1164 12월  6 16:46 snort.log.1638776809
-rw------- 1 root root 6840 12월  6 17:23 snort.log.1638777544
-rw------- 1 root root 1164 12월 14 17:57 snort.log.1639472245
[root@isec snort]# tcpdump -r snort.log.1639472245
reading from file snort.log.1639472245, link-type EN10MB (Ethernet)
17:57:30.227224 IP 192.168.183.129 > isec: ICMP echo request, id 15731, seq 1, l
ength 64
17:57:30.227270 IP isec > 192.168.183.129: ICMP echo reply, id 15731, seq 1, len
gth 64
17:57:31.230972 IP 192.168.183.129 > isec: ICMP echo request, id 15731, seq 2, l
ength 64
17:57:31.231135 IP isec > 192.168.183.129: ICMP echo reply, id 15731, seq 2, len
gth 64
17:57:32.234391 IP 192.168.183.129 > isec: ICMP echo request, id 15731, seq 3, l
ength 64
17:57:32.234489 IP isec > 192.168.183.129: ICMP echo reply, id 15731, seq 3, len
gth 64
```